# YEAR 2000 SYSTEMS COMPLIANCE TESTING AND CONTINGENCY PLANNING FOR BUSINESS CONTINUITY AT THE DEPARTMENT OF THE TREASURY

OIG-00-025 December 29, 1999

Office of Inspector General

*******

United States Department of the Treasury

**DEPARTMENT OF THE TREASURY**
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

DEC 29 1999

MEMORANDUM FOR NANCY KILLEFER
ASSISTANT SECRETARY FOR MANAGEMENT
AND CHIEF FINANCIAL OFFICER

FROM: Dennis S. Schindel Dennis Schindel
Assistant Inspector General for Audit

SUBJECT: Year 2000 Systems Compliance Testing and Contingency Planning for Business Continuity at the Department of the Treasury

This memorandum transmits our final report on our evaluation of the Department of the Treasury's (Department or Treasury) oversight of Treasury bureau Year 2000 (Y2K) compliance testing of systems and contingency planning for business continuity. Our report also discusses the Department's planning efforts for "Day One" reporting of its Y2K status to the President's Council on Year 2000 Conversion (President's Y2K Council).

Our review disclosed that the Department needs to ensure that all Treasury Communications System (TCS) equipment is adequately tested and is Y2K compliant. We also found that the Y2K status reports submitted by Treasury bureaus we reviewed did not always reflect accurate and complete information pertaining to the Y2K testing and certification status of Treasury systems. Additionally, weaknesses were noted in testing procedures and Y2K project management at these bureaus.

While Treasury bureaus have made notable progress to develop and test business continuity and contingency plans (BCCP), significant work remains to finalize these plans before the year 2000. Therefore, the Department needs to more closely monitor these remaining tasks so that it can be assured essential services will be provided in the event of Y2K-induced failures of mission-critical systems.

We are also reporting that the Department made significant progress to implement a "Day One" strategy for reporting on the Y2K status of core business processes and mission-critical systems to the President's Y2K Council during the century rollover period. Additionally, the Department has taken steps to ensure that senior Treasury officials are aware of their roles and responsibilities for Y2K issues. Further tests, however, are needed to ensure the full functionality of the Department's Emergency Information Coordination Center (EICC) as well as the backup facility for the EICC.

In our report, we recommend that the Department follow up on: (1) the Y2K readiness of the TCS; (2) the weaknesses in Y2K compliance testing and project management identified at the bureaus we reviewed; and (3) the status of bureau BCCPs, including testing of these plans. Additionally, the Department needs to ensure that the full functionality of the EICC and its backup facility is adequately tested.

In your December 16, 1999, response to our draft report, you did not concur with our recommendations related to the TCS and the need to follow up on the bureau Y2K compliance testing and project management weaknesses we identified. Your response, which is summarized and evaluated in the body of the report and included as Appendix 2, also objected to certain other matters. Based on our review of the bases cited for your non-concurrence and our audit work, we believe our findings and conclusions are valid and the recommendations appropriate. Therefore, we strongly encourage the Department to reconsider its position with respect to the non-concurred recommendations. Because of the very limited time remaining until the year 2000 to address our findings, we are issuing this report as final without further discussion of the disagreements.

Please be advised that it is the Office of Inspector General's policy to make our reports available to the public. However, at the request of your staff, we will limit the distribution of this report to the individuals identified in Appendix 4 and to the U.S. General Accounting Office until after December 31, 1999.

We will be entering the recommendations contained in this report in the Inventory Tracking and Closure (ITC) System. Consistent with Treasury Directive No. 40-01, we request a written description of actions taken and planned, and target dates for any incomplete corrective actions, within 30 days of the date of this memorandum.

We appreciate the courtesies and cooperation provided to our auditors during the review. If you wish to discuss this report, you may contact me at (202) 927-5400 or a member of your staff may contact Clifford Jennings, Director of Information Technology Audits, at (202) 927-5240.

Attachment

## Table of Contents

Appendices

# Overview

We evaluated the Department of the Treasury's (Department or Treasury) oversight of Treasury bureau Year 2000 (Y2K) compliance testing of systems and contingency planning for business continuity. We also evaluated the Department's planning efforts for "Day One" reporting of its Y2K status to the President's Council on Year 2000 Conversion (President's Y2K Council). This is the third review by our office of the Department's Y2K conversion effort.

Our first review, conducted during January and February 1998, primarily focused on the Department's Y2K assessment activities. In our second review, conducted from April through September 1998, we evaluated Y2K project management, the systems conversion and certification process, and contingency planning at 11 bureaus. The results of these reviews were reported to the Assistant Secretary for Management and Chief Financial Officer.[1]

Our current review disclosed, as a particular concern, the Treasury Communications System (TCS). Specifically, the Department needs to ensure that TCS equipment is adequately tested and is Y2K compliant. Unreconciled discrepancies between two TCS equipment inventory listings raise questions whether all TCS equipment needing Y2K testing has in fact been identified and tested.

Our current review identified two other issues that need to be followed up by the Department as part of its management of the Y2K conversion effort. Specifically, the information pertaining to the Y2K testing and certification status of Treasury systems in status reports submitted by the bureaus we reviewed was sometimes incomplete or inaccurate. We also found weaknesses in testing procedures and Y2K project management at the bureaus.

Additionally, while Treasury bureaus have made notable progress to develop and test business continuity and contingency plans (BCCP), significant work remains to finalize these plans before the year 2000. Therefore, the Department needs to more closely monitor the

[1] *The Department Met the Year 2000 Compliance Indicators for Fiscal Year 1997* (OIG-98-090; issued May 27, 1998) and *Year 2000 Compliance Efforts at the Department of the Treasury* (OIG-99-103, issued August 6, 1999).

remaining contingency planning tasks so that it can be assured essential services will be provided in the event of Y2K-induced failures of mission-critical systems.

The Department has made significant progress to implement a Day One strategy for reporting on the Y2K status of mission-critical information technology (IT) and non-IT systems to the President's Y2K Council during the century rollover period. For example, the Department established and performed limited tests of its Y2K Emergency Information Coordination Center (EICC). Additionally, the Department has taken steps to ensure that senior Treasury officials are aware of their roles and responsibilities for Y2K issues. Further tests, however, are needed to ensure the full functionality of EICC operations as well as the Department's backup facility for the EICC.

As a concluding observation, the oversight exercised by the Department during the Y2K conversion process has primarily been that of: (1) issuing policy and guidance to the bureaus; and (2) collecting, consolidating, and forwarding information to the Office of Management and Budget (OMB) on the status of the bureaus' Y2K efforts. Collectively, we believe the conditions we have identified in this report demonstrate the need for increased oversight by the Department. Given the very limited time left before the year 2000, the Department needs to identify what risks remain with system renovation efforts as identified in this report, provide assistance as necessary to reduce those risks, and ensure adequate contingency plans are in place to continue essential operations in the event of unforeseen internal and external failures.

Accordingly, we are recommending in this report that the Department: (1) follow up on the identified issues with bureau Y2K status reporting, testing procedures, and project management; (2) ensure <u>all</u> TCS equipment is Y2K compliant; (3) obtain and validate information on the status of bureau contingency planning efforts and, as necessary, provide assistance to ensure essential services will continue in the event of Y2K-induced failures; and (4) ensure sufficient tests are made of EICC operations before Day One, including tests of the EICC backup facility.

In a written response to our draft report, the Assistant Secretary for Management and Chief Financial Officer disagreed with our characterization of the Department's oversight exercised during the Y2K conversion process and stated that the Department has been very actively engaged in the Y2K program efforts by the bureaus for over 3 years. Management also did not concur with our recommendations to follow up on identified issues related to: (1) bureau Y2K status reporting, testing procedures, and project management; and (2) the TCS. With regard to the TCS, management stated that all critical, date/time sensitive equipment was adequately tested and is Y2K compliant. Management concurred with our recommendations related to bureau contingency planning efforts and EICC operations. Based on our review of the bases cited for the non-concurred recommendations and our audit work, we believe our findings and conclusions are valid and the recommendations appropriate. Management's comments to the non-concurred recommendations are summarized in the body of this report and the complete text of the response is included as Appendix 2.

## Objective, Scope, and Methodology

We initiated this review to more closely evaluate selected aspects of the Department's oversight of bureau Y2K conversion efforts. Our specific objectives were to evaluate the accuracy of bureau reporting to the Department and by the Department to OMB on the status of (1) system certification for Y2K compliance and (2) business continuity and contingency planning and testing of contingency plans. We also evaluated the Department's Day One strategy to collect, analyze, and summarize information on the status of core business processes and mission-critical systems during the century rollover period and other dates associated with the Y2K problem. Using a risk-based approach, we focused our review on those bureaus and Treasury offices whose mission-critical systems have the greatest impact to the public and Treasury operations. These bureaus and offices were: United States Customs Service (Customs); Bureau of Alcohol, Tobacco and Firearms (ATF); Financial Management Service (FMS); Bureau of Public Debt (BPD); Bureau of Engraving and Printing (BEP); the United States Mint (Mint); and Corporate Systems Management (CSM).

We coordinated our work at Customs and FMS with the U.S. General Accounting Office (GAO). At the time we began our work at Customs, GAO was evaluating Customs' role as the lead Federal agency for assuring the Y2K readiness of the Cross-border Inspection Services program, one of 43 Federal programs designated has high impact by OMB. We discussed our objectives with the GAO auditors and concluded that the scope of their work with respect to contingency planning was essentially similar to ours. Also, GAO had reported in March 1999 that Customs had established effective Y2K program controls. Although important Y2K work remained to be accomplished by Customs at the time, including validation of contingency plans, the GAO report stated that Customs had plans in place for completing key tasks, and the management controls to ensure that they were accomplished.[2] Accordingly, we did not make any further inquiries during this review with respect to Customs' Y2K contingency planning efforts. At FMS, GAO was reviewing FMS' management controls over Y2K systems compliance testing. Accordingly, our inquiries with respect to compliance testing were limited to the information provided by FMS in its monthly status reports to the Department.

To accomplish our objectives, we interviewed: (1) the Department's Year 2000 Program Manager and key staff of the Office of the Deputy Assistant Secretary for Information Systems and Chief Information Officer; and (2) as appropriate, bureau Y2K project management staff and contractor personnel. We also reviewed: (1) prior GAO and Office of Inspector General (OIG) reports related to Y2K conversion at Treasury bureaus; (2) the May 21 and August 23, 1999, quarterly status reports submitted by the Department to OMB; (3) monthly status reports submitted by the bureaus to the Department through the month of September 1999; (4) selective documentation of the above bureaus supporting the status reporting of systems testing and contingency planning efforts; and (5) available policies, procedures, and training materials for the Department's Day One strategy. Additionally, we observed an EICC table top training exercise in August 1999 and a test of EICC operations conducted in October 1999. In determining the adequacy and reasonableness of documentation we reviewed, we considered Y2K testing, contingency

[2] *Year 2000 Computing Crisis: Customs Has Established Effective Year 2000 Program Controls* (GAO/AIMD-99-37; issued March 29, 1999).

planning, and Day One planning guidance issued by GAO.[3] OMB and the Department have generally adopted this guidance as policy for agency Y2K project management.

We started our fieldwork in May 1999. Because of the need to provide our audit results and recommendations to the Department in order for it to take corrective action within the limited time remaining before January 1, 2000, we ended our fieldwork on November 8, 1999, and provided our initial draft of this report to the Department's Year 2000 Program Manager on November 12, 1999. In some instances, we did not obtain and analyze all supporting documentation to corroborate verbal and written information on the status of testing and contingency planning efforts by this date. As a general observation, efforts to complete system renovations and develop, test, and validate contingency and Day One plans were on-going during our review and, in some instances, are scheduled for completion through December 1999. However, we believe the work that we performed supports the conclusions and recommendations included in this report.

The objective of our evaluation was not to determine whether any given Treasury system is Y2K compliant or that a system will work into the next millennium. Accordingly, we do not provide such assurance.

We conducted our audit in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States, and included such audit tests as were deemed necessary.

## Audit Results

### Additional Measures Are Needed To Ensure The Reliability Of Information Used To Manage The Y2K Conversion

The information reported by each of the Treasury bureaus is intended to report the current status of the conversion and certification of all Treasury systems. However, the Department does not independently

[3] *Year 2000 Computing Crisis: A Testing Guide* (GAO/AIMD-10.1.21; issued in November 1998); *Year 2000 Computing Crisis: Business Continuity and Contingency Planning* (GAO/AIMD-10.1.19; issued in August 1998); and *Y2K Computing Challenge: Day One Planning and Operations Guide* (GAO/AIMD-10.1.22; issued in October 1999).

validate or verify information that it uses to monitor the conversion effort and which is reported in periodic Y2K status reports to OMB. As a result, the Department does not have assurance that Treasury's mission-critical systems were adequately tested and are actually compliant and that its systems will function as intended in the next century.

OMB requires Federal agencies to provide quarterly reports on their progress in making systems Y2K compliant. OMB reporting guidance also requires that department heads take steps "to assure independent verification that systems are fixed and to assure that information reported is accurate."[4] At Treasury, the bureaus are required to report their progress monthly to the Department. The Department uses the information reported by the bureaus to monitor each bureau's Y2K conversion effort and to compile the overall Treasury reports submitted to OMB quarterly.

During our review, we noted that some verification efforts are being performed by the various bureaus. These verification efforts are reported monthly by the bureaus and consolidated in Treasury's quarterly progress report to OMB. For example, bureaus like the BEP, ATF, and FMS have contracted with outside organizations to conduct independent verification and validation (IV&V). Similarly, other bureaus have chosen to perform their own IV&V by bureau component organizations that were not directly involved with system renovation. These verification efforts, if performed as reported by the bureaus, serve as the final confirmation that systems, which have been renovated and tested for Y2K compliance, are actually compliant. It would also provide an additional level of assurance that system renovation is complete. However, during our review we found that these IV&V efforts reported in the bureaus' monthly status reports were not always accurate, consistent and complete. In addition, we found some weaknesses in testing procedures and Y2K project management at the bureaus.

[4] OMB Memorandum M-99-21, *Revised Reporting Guidance on Year 2000 Efforts*, dated August 6, 1999.

### Inaccurate and Incomplete Year 2000 Reporting by Treasury Bureaus

During our review, we found that significant information pertaining to the Y2K conversion effort was not included in monthly status reports and was sometimes misleading and/or inaccurate for the bureaus reviewed. We found instances where mission-critical systems were omitted from reporting and that IV&V testing processes were not always as thorough as reported. Also, bureau reports contained inconsistencies or Y2K status was not reported formally but verbally instead. These conditions are described below:

- <u>ATF</u>. ATF did not report the conversion efforts of all mission-critical systems in its monthly status reports. ATF's Y2K conversion plan incorporates their planned effort to also migrate ATF mainframe legacy systems to a client-server environment. Therefore, as ATF renovates mainframe systems to client-server versions, Y2K changes are made simultaneously. For most of ATF's mission-critical systems, the status of the client-server versions was reported in the Y2K status reports. However, ATF reported the status of the mainframe versions for two of its mission-critical systems instead of the client-server versions. These two systems are the Financial Management Information System (FMIS) and the Simplified Time and Attendance Tracking System (STATS).

  The replacement systems for the FMIS and STATS systems were originally due for implementation by October 1, 1999. However, ATF is now targeting December 1999 for implementation of the FMIS and STATS replacement systems. ATF performs IV&V of systems after systems are implemented. This differs from the recommended five phase approach outlined in GAO's Year 2000 Conversion Model where it is recommended that IV&V be performed before a system is implemented. While ATF's approach allows the end-user earlier usage of the system, it poses additional risk for the FMIS and STATS replacement systems. ATF's IV&V contractor stated that the FMIS replacement system is heavily date dependent containing approximately two thousand date fields and estimated that it would take 2 months to complete IV&V. If ATF meets its estimated implementation date of December 1999 for the replacement FMIS and STATS systems, IV&V testing will not be completed before January 1, 2000. The Department may not be aware of the increased risk in system malfunctions in the year 2000 of the FMIS and STATS replacement systems because this information is not reported in ATF's Y2K status reports.

In another instance, detail pertaining to an ATF mission-critical system was not included in the bureau's status reports because the system, N-Force, was categorized as non-mission-critical when the system owners believe that the system is mission-critical. The N-Force system is being developed to incorporate three existing ATF mission-critical systems in a phased approach. The conversion and testing of the three N-Force component systems: Form for Criminal Investigation system (Form 3100), Form for Property Inventory/Forfeiture Property Appraisal Report (Form 3400), and the Criminal Enforcement Management Information System, are reported in the ATF status reports in their separate, stand alone state. Detail pertaining to the development and testing of N-Force is not included in the monthly status reports. Although N-Force is currently in production and was certified by the IV&V contractor as "Year 2000 Ready", we believe ATF should re-categorize N-Force as a mission-critical system in order for the Department to be aware of the system's detailed development status and ensure the system receives priority in the event failures occur in the next century.

- BEP. At BEP, a contractor was retained to perform IV&V work on the bureau's mission-critical computer systems. The contractor was unable to perform what it considered to be IV&V, and stated in its March 1999 report: "IV&V testing is not possible." As part of the IV&V process, the contractor requested pre-renovated system code in order to analyze the renovation process. The bureau was unable to provide the contractor with the pre-renovated code as well as documentation describing the changes that were made to the systems. BEP's monthly status report to the Department was incomplete because it failed to notify the reader of the contractor's statement that IV&V was not possible. The contractor did perform elements of an IV&V, including a code review. However, a code review falls short of certifying the renovation process.

- Mint. The Y2K status reporting at the Mint was incomplete and inaccurate. As discussed in previous OIG reports, the Mint reported in its April 8, 1999, status report to the Department that all mission-critical systems and external interfaces had been successfully tested and implemented into the production environment.[5] However, systems were only tested to determine whether they could process data properly and did not include specific tests for Y2K compliance. The May 7, 1999, status report mentioned matters of concern such as the IV&V Test Suite, which is the facility used to simulate date conditions for any of the critical dates associated with the millennium rollover, not being operational. The report did not provide other necessary detail including that the Mint had fallen behind in meeting its testing milestones; details on how many systems needed to be tested; and the exact date the Mint expected to start testing. However, according to a July 8, 1999, monthly status report, new milestone dates were introduced. This included both start and finish dates for IV&V testing.

- FMS. The FMS status report for the month of September 1999 contained inconsistent information. The total number (16) of mission-critical non-IT systems subject to Y2K conversion did not reconcile with the number reported (23) in the Year 2000 Data Element Status Assessment table. Also, in the narrative section of the report for non-IT systems, the status information did not reconcile with the numbers identified in the Non-IT Year 2000 Data Element Status Assessment table. In addition, FMS cited that at the end of October 1999, the Claims and Courtesy Disbursement systems were scheduled for implementation at two remaining financial centers. However, an Independent Validation and Verification Process Status report dated November 2, 1999, showed that the systems were still being prepared for implementation.

- TCS. The information in an October 19, 1999, memorandum from the Department to OMB concerning the status of the TCS was not accurate. TCS is a mission-critical, general support automated

[5] *Year 2000 Compliance Testing and Contingency Planning for Business Continuity at the United States Mint* (OIG-99-110; issued August 24, 1999) and *Monitoring of the United States Mint's Year 2000 Systems Compliance Testing and Contingency Planning for Business Continuity* (OIG-99-114); issued August 24, 1999).

information system that is to provide cost effective communications between more than 6,500 Treasury, Government, and commercial locations in the United States, its Territories, and internationally. The TCS provides communications services and a full range of network and information technology products and services to meet the mission needs of Treasury, its bureaus, and its offices. In their memorandum to OMB, Treasury stated that, for the TCS:

> "...Installation of Year 2000 compliant equipment...will be completed by November 1999...Approximately 95% of the scheduled remediations have been completed."

However, on October 20, 1999, the OIG reviewed an internal TCS schedule that showed specific Treasury users, such as for the Executive Office for Asset Forfeiture, where the TCS equipment was not projected to be Y2K compliant on January 1, 2000. Additionally, the inventory of scheduled remediations includes only those that have been approved by the bureaus. Remediations not performed due to the existence of a waiver or lack of bureau approval are not included in the calculation of remediations completed.

The bureaus and other TCS users also need detailed information about the Y2K status of the TCS equipment. The Y2K status of TCS equipment at each location is necessary for the TCS users to decide whether to rely on the TCS after the year 2000 date change. However, detailed TCS Y2K information is not being provided in a usable form. The TCS users are being supplied with inventory reports that are often too voluminous to be useful. Additionally, TCS users have reported difficulties in accessing a TCS web site with the Y2K status of TCS equipment. Without timely access to this information, the TCS users may not be aware of the location of the 20 percent of the TCS inventory that CSM has listed as not Y2K compliant.

### Weaknesses in Testing Procedures and Year 2000 Project Management

We identified weaknesses in Y2K testing procedures and project management at the bureaus reviewed. These weaknesses include compliance testing procedures, change management, and IV&V procedures. In addition, we found that the responsibility for ensuring Y2K compliance of some equipment that may be affected by the century rollover has not been assigned. These conditions are described below:

- ATF. We found that Y2K compliance testing was not performed on all ATF mission-critical systems. In addition, compliance testing documentation was not available for some mission-critical systems that ATF reported as tested. The testing documentation that was available for our review was often incomplete, indicating that the testing performed may have been inadequate. The risk of Y2K-induced system failures which is posed by ATF's compliance testing is somewhat mitigated because ATF established an IV&V process. However, ATF's policy is that each system undergoes IV&V testing only once. The risk of system failures is not mitigated by the IV&V process when system changes are made subsequent to the IV&V certification.

  As part of our review at ATF, we requested a list of changes made to systems subsequent to IV&V certification. We also requested that ATF provide documentation to show that these systems were regression tested to ensure Y2K compliance after the changes were made. However, this information was not readily available and ATF was unable to provide this documentation. ATF indicated in a written response to our request that:

  > "...it is ATF's practice to verify all changes made to baseline systems to ensure the desired effects are realized. However, support documentation is not maintained."

- Customs. Along similar lines as ATF, Customs was unable to provide documentation that we requested for review. While Customs has a strong Y2K effort, we are concerned that they were unable to produce documentation that all modules of their six critical systems had been processed through their automated IV&V tool, CCD Online.

- BPD. BPD identified five mission-critical IT systems, all of which have been certified by the bureau as Y2K compliant. Part of the remediation process recommended by the GAO to achieve Y2K compliance includes IV&V of IT systems. BPD utilized the same personnel to perform IV&V tasks as those initially assigned to repair the computer code. Although this practice does provide some assurance that the systems were renovated for the year 2000, it does not meet the standard of performing an independent verification and validation of the Y2K conversion effort.

- TCS. There are components of the TCS that are not part of a Y2K remediation plan. CSM, a part of Treasury's Departmental Offices, is the program office responsible for the TCS. CSM has accepted ownership and responsibility only for telecommunications equipment (1) which has been purchased by its prime contractor under the TCS contract and (2) for which a maintenance fee is being paid. CSM has not accepted ownership and responsibility for all TCS equipment purchased by the Department's telecommunications Working Capital Fund, especially items purchased under the Consolidated Data Network (CDN) contract.

The inventory of TCS equipment under maintenance includes 12,767 line items, whereas a fiscal year 1999 billing inventory of all TCS equipment includes 88,803 line items. This larger inventory includes items for which the year change will have no impact, such as "racks." However, this inventory also includes older TCS equipment, for example routers, which may be affected by the date change. This older equipment is not part of a TCS Y2K remediation plan because Treasury bureaus have not funded maintenance of this equipment or have not approved Y2K upgrades.

All TCS equipment has not been tested as individual components or in a network configuration. TCS users are relying on CSM to ensure that all TCS equipment has been tested. However, CSM has not completed component testing of all TCS equipment. CSM has also placed responsibility for network configuration testing of TCS equipment on the TCS users. Only ATF and the Departmental Offices have performed this level of testing. During our exit briefing with Departmental officials, we were told that the entire TCS system could not be taken off line for testing. However, there was little concern of failure as all component types, which had been identified by the system management software, had been tested.

### Conclusion

Accurate and complete status reporting by the bureaus is needed in order for the Department to effectively manage the overall Y2K conversion effort. As described in the conditions above, we determined that information in monthly status reports for the bureaus reviewed was sometimes incomplete or inaccurate. In addition, some Treasury systems may be at risk of failure due to weaknesses in Y2K testing procedures and project management at the bureaus. Because the Department does not have complete and reliable information about the bureaus' Y2K conversion status, the Department lacks assurance that all Treasury systems reported as Y2K compliant will function in the next century. In addition, the Department does not have assurance that systems which have been certified as Y2K compliant have not been degraded by maintenance and system changes.

### Recommendations

1. The Deputy Assistant Secretary for Information Systems and Chief Information Officer should follow up to ensure that the issues with bureau Y2K status reporting, testing procedures, and project management identified above are appropriately resolved.

   Management Response and OIG Comment

   The Department did not concur with this recommendation. The Department responded that, prior to the OIG's second audit of the Department's Y2K effort, performed during April through September 1998, its Y2K contractor was responsible for conducting bureau assessments of the Y2K conversion progress and reporting reliability. Once the OIG began its review, the Department redirected its Y2K contractor to focus on providing guidance on external interfaces, end-to-end testing, and the Business Continuity and Contingency Planning. In addition, the Department expected that the assessments made by the OIG would be provided on a timely basis to validate the data submitted to the Department for each OMB report.

The Department is non-responsive to the recommendation and provides no explanation as to why no follow-up should be performed on issues identified relating to status reporting, testing procedures, and project management.

2. The Deputy Assistant Secretary for Information Systems and Chief Information Officer should direct CSM to ensure all TCS equipment and property purchased by the telecommunications Working Capital Fund for the TCS or prior programs has been adequately tested and is Y2K compliant. CSM's efforts should be closely monitored to ensure all appropriate actions are taken.

   Management Response and OIG Comment

   The Department did not concur with this recommendation. In its response, the Department stated that CSM ensured all critical, date/time sensitive equipment purchased by the telecommunication Working Capital Fund for the TCS or CDN programs were adequately tested and are Y2K compliant. CSM took steps to address all critical TCS equipment, including items purchased under the predecessor CDN contract. Further, all relevant equipment was tested as individual components, as a thread of components used in their network context, and a part of a representative network segment. The Department is confident that they have an accurate database of all TCS equipment, and have performed the proper assessment of the equipment in that database as it relates to this Y2K compliance issue.

   Based on our audit work and discussions held with you and your staff on November 30, 1999, regarding our discussion draft of this report dated November 12, 1999, we believe the issues with the testing and Y2K compliance of TCS equipment as outlined in our finding are valid. Accordingly, we believe management should implement this recommendation.

3. The Deputy Assistant Secretary for Information Systems and Chief Information Officer should instruct CSM to immediately provide: (a) a written status report detailing the Y2K conversion progress of the TCS; and (b) the bureaus and the users of the TCS, in electronic format, the compliant/non-compliant status of the TCS equipment installed at their specific locations so as to facilitate the

bureaus' ability to understand the Y2K status of their TCS equipment.

Management Response and OIG Comment

The Department did not concur with this recommendation. CSM and the TCS program office provided written status reports and updates detailing the Y2K conversion process for over 18 months. These reports have been provided to each bureau at Total Quality Management/Information Sharing Session meetings, Bureau Y2K Meetings, and other forums. All bureaus have been informed of the TCS Y2K compliance status along the way. As of November 30, 1999, the TCS network is fully Y2K compliant. Each bureau is aware of their individual TCS/Y2K status.

Based on our audit work, we believe the issues with the testing and Y2K compliance of TCS equipment as outlined in our finding are valid. Accordingly, we believe management should implement this recommendation.

### Increased Oversight of Bureau Y2K Contingency Planning Efforts And Additional Testing Of "Day One" Strategy Is Needed

While Treasury bureaus have made notable progress to develop and test BCCPs, significant work remains to finalize these plans before the century rollover. Therefore, the Department needs to more closely monitor the remaining contingency planning tasks so that it can be assured essential services will be provided in the event of Y2K-induced failures of mission-critical systems.

The Department has also made significant progress to implement a Day One strategy for reporting on the Y2K status of mission-critical IT and non-IT systems to the President's Y2K Council during the century rollover period. For example, the Department established the Year 2000 EICC and performed a limited "dry run" of EICC operations on October 7, 1999, to test its automated tool for collecting, analyzing, and summarizing information on the status of core business processes and mission-critical systems. Furthermore, the Department has taken steps to ensure that senior Treasury officials are aware of their roles and responsibilities for Y2K issues. Additional tests, however, are needed to ensure the full functionality of EICC operations.

### Business Continuity and Contingency Planning

Treasury bureaus have reported that, for the most part, mission-critical systems have been renovated and tested to address the Y2K problem. Nevertheless, because core business processes of the Department may still be disrupted by Y2K-induced failures in internal systems, business partners' systems, or public infrastructure systems, it is necessary that the Department ensure contingency plans are developed and tested for the continuity of business operations. If done effectively, such plans can help mitigate the risks and mission impacts associated with unexpected internal and uncontrollable external system failures.

In its various Y2K directives, OMB has not established specific target dates for agencies to have prepared and tested BCCPs. In testimony before the House Committees on Government Reform and on Science during January 1999, GAO suggested that OMB consider setting target dates such as: (1) April 30, 1999, to complete BCCPs for core business functions; and (2) September 30, 1999, to complete testing and validation of agency business continuity strategies.[6] Although these target dates have not been mandated, they provide a useful benchmark to measure where bureaus should be at, given the limited time remaining before the century rollover, in order for the Department to be assured that bureau BCCPs will work if they are needed.

In its instructions for preparing required quarterly reports due August 13 and November 15, 1999, OMB requested information on the progress to develop and test BCCPs. This information is to include: (1) assurances that local and regional offices (i.e., Treasury bureaus) have developed and tested BCCPs in coordination with the Department; and (2) the total number of such offices (i.e., Treasury bureaus) which require BCCPs and the number that have such plans in place.[7] To assist the Department in formulating the quarterly Y2K

[6] *Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions* (GAO/T-AIMD-99-50; January 20, 1999).

[7] OMB Memorandum M-99-21, *Revised Reporting Guidance on Year 2000 Efforts*, dated August 6, 1999.

report to OMB, the Department requires each bureau to submit monthly status reports.

The Department's most recent quarterly report to OMB, dated August 23, 1999, provided only general information on the progress of the Department's contingency planning efforts. Specifically, the Department reported that bureau enterprise-level BCCPs had been reviewed and that recommended changes were implemented.[8] The report also stated that the Department anticipated that all bureaus would complete testing of their BCCPs by October 1999—the time frame recommended by GAO.

We reviewed the status reports submitted by 13 bureaus and other Treasury offices for the month of September 1999.[9] As a general observation, the reports did not provide the Department sufficiently detailed information to effectively assess the bureaus' progress in developing and testing BCCPs. For example, the bureaus did not report on the status of contingency planning in a consistent manner. The status reports for eight bureaus did not indicate whether contingency plans had been tested or, if tested, when the testing had occurred. The status reports for two bureaus, however, indicated that testing of their contingency plans had not been initiated as of September 30, 1999.

Our more in-depth reviews at 4 bureaus and offices found that for 3 of the reporting entities, significant work still remained to complete contingency plans and to test and validate contingency strategies, as discussed below:

- ATF. ATF developed contingency plans for its 24 IT mission-critical systems. Our review of 7 of the plans found that while they

[8] According to GAO Y2K contingency planning guidance and related OMB directives, agencies should develop BCCPs for (1) the agency as a whole (i.e., an "enterprise-level" BCCP), (2) each core business process, and (3) each infrastructure component, or system, supporting the core business processes. While the Department substantively reviewed the enterprise-level BCCPs of the bureaus for conformance with GAO's guidance, it did not require bureaus to provide the more detailed contingency plans for each core business process and supporting mission-critical systems.

[9] The Internal Revenue Service (IRS) also submits monthly status reports to the Department. The Treasury Inspector General for Tax Administration has the audit responsibility for IRS. Accordingly, the IRS was not included in the scope of our review.

generally conformed to ATF's guidance, they did not include certain elements contained in GAO's guidance. During our audit, we provided our observations on these plans to the ATF's Y2K Program Management Office (PMO). We also noted that ATF had not developed contingency plans for its six core business processes and provided this feedback to the PMO in July 1999. Subsequently, ATF established an October 21, 1999, target date for the core business process owners to develop these plans. However, as of November 2, 1999, the plans were still being developed, according to PMO staff.

ATF still needs to test and validate its contingency strategies. In September 1999, the PMO issued guidance for developing contingency test plans and in October 1999, ATF's Y2K Senior Executive discussed the testing plan, methodology, and testing schedule with the executives responsible for each core business process. ATF plans to have testing and validation of contingency plans completed by December 1999.

- FMS. FMS' Y2K Special Projects Office (SPO) had issued appropriate guidance for preparing and testing contingency plans. It has also engaged a contractor to review the contingency plans and related test plans prepared for FMS' business lines and supporting mission-critical systems.[10] However, documentation supporting contingency planning efforts was incomplete at the time of our review, and further tests are scheduled through December 1999 to validate the plans.

  In its September 1999 status report to the Department, FMS reported that testing of contingency plans was expected to be completed by the Fall of 1999 for its business lines and by November 30, 1999, for its mission-critical systems. The status report did not provide quantitative information as to the number of offices that require BCCPs and the number that had such plans in place. However, FMS reported that about 88 percent of mission-critical contingency test plans had been received and reviewed by the SPO. Internal SPO tracking reports showed that as of

[10] FMS has four business lines: Payments and Claims, Collections, Accounting and Reporting, and Debt Collection. These business lines are supported by a total of 58 mission-critical systems.

November 5, 1999, system contingency plans had been tested and validated for 22 of 58 mission-critical systems. For the remaining 36 system contingency plans, testing had either not been scheduled (3 plans) or was scheduled for varying periods through the end of December 1999 (33 plans). The contingency plans still to be tested were primarily related to FMS' Payments and Claims business line and included the systems to process social security (SSA), supplemental security income, and tax refund payments. Thus, the SPO internal tracking reports indicates that substantial testing remained to validate contingency plans.

FMS disbursement officials told us, during an oral briefing on November 4, 1999, that more extensive testing had occurred on the Payments and Claims contingency plans than was indicated on the SPO internal tracking reports, although further tests were planned in November and December 1999. For example, FMS had made extensive preparations—in coordination with Federal program agencies, the Federal Reserve Bank, and the United States Postal Service—to process and deliver critical payments due in early January 2000, such as those to SSA recipients. Other major Federal recurring payments, such as those for Office of Personnel Management programs, are due later in January. Therefore, FMS will have time, although limited, after the century rollover to address any Y2K impacts to payment delivery systems before these payments are due.[11] According to FMS disbursement officials, various contingency plans for payment processes have also been tested as part of FMS' normal course of business. For example, payments for a major Federal program are generally processed by the same FMS regional financial center each payment cycle (e.g., SSA payments are normally processed by FMS' Philadelphia center). FMS has the capability to shift normal processing to another regional center if necessary (e.g., SSA payments can be processed by FMS' Hyattsville center). FMS officials acknowledged that documentation of contingency plans for payment systems, as well as testing of plans, was incomplete

[11] It should also be noted that GAO reported in October 1999 that FMS had established effective Y2K test management controls for its six most mission-critical systems including the payment systems for social security, supplemental security income, and tax refunds (*Year 2000 Computing Challenge: Financial Management Service Has Established Effective Year 2000 Testing Controls* (GAO/AIMD-00-24; October 29, 1999)). According to FMS disbursement officials, the lines of code involving date computations and requiring renovation were minimal in the application software for these payment systems.

and that existing plans need to be updated to reflect FMS' current operating environment.

- TCS. CSM has made substantive progress in developing and testing the contingency plan for TCS. However, critical testing activities still must be completed to validate the plan. For example, a walk through of the TCS contingency plan with the bureau representatives is scheduled for November 30, 1999, so that the bureau representatives are familiar with procedures, roles, and responsibilities. However, a planned walk through with TCS management had not yet been scheduled. In addition, while TCS addressed its needs for critical staffing to carrying out the contingency plan, staffing by its vendors is still to be addressed by those organizations. We were told by TCS staff that its prime contractor, in conjunction with Treasury, plans to ensure that these outside organizations will be ready.

The latest status report submitted to the Department by BPD in which it specifically discussed the status of contingency planning efforts was for the month of February 1999. In that report, BPD stated that contingency plans had been documented for its five IT mission-critical systems. BPD also stated that it had substantial recovery planning documents that describe how each of its offices would react in the event an emergency and that these plans were being updated for potential Y2K problems. According to BPD, the plans had been subjected to testing exercises. We found that BPD's enterprise-level BCCP generally conformed to GAO guidance. According to the BPD Y2K Project Manager, BPD had completed testing and updating of its contingency plans. BPD was also in the process of incorporating its Day One plan in the enterprise-level BCCP. Due to the timing of our audit work, we did not review BPD's supporting documentation of these efforts.

During our audit, we also reviewed contingency planning efforts at the Mint and issued separate reports to the Mint Director and to the Assistant Secretary for Management and Chief Financial Officer on August 24, 1999. We reported that the Mint's enterprise-level BCCP, dated May 14, 1999, generally conformed to GAO guidance. However, the Mint still needed to complete contingency plans for its five Strategic Business Units

(SBU) and supporting mission-critical systems.[12] In a memorandum dated October 8, 1999, the Mint Director advised that the Mint had completed contingency planning for the SBUs and mission-critical systems, and had completed testing of the contingency plans for the mission-critical systems and mission-critical functions within its Circulating and Numismatic SBUs.

### Day One Planning

According to GAO guidance, a Day One strategy comprises a comprehensive set of actions to be executed by a Federal agency during the last days of 1999, the first days of 2000, and other Y2K-impacted dates such as February 29, 2000. The Day One strategy should be integrated with agency business continuity and contingency plans, and should describe the key activities and responsibilities of agency component organizations and staff. The objectives of a Day One strategy are to: (1) position an organization to readily identify Y2K-induced problems, take needed corrective actions, and minimize adverse impact on agency operations and key business processes; and (2) provide information about an organization's Y2K condition to executive management, business partners, and the public.[13]

The Department has been proactive in developing plans to monitor the status of mission-critical systems during Day One and other key dates associated with the century rollover and, if necessary, to determine a course of action in the event of Y2K-induced failures of core business processes and mission-critical systems. Specifically, it has established the EICC to collect, analyze, and disseminate information to senior Treasury executives and the President's Y2K Council. The Department has performed limited tests of EICC operations and further tests are planned before year-end. The Department also plans to set up a fully functional backup site for the EICC at another Treasury facility. Additionally, it has ensured that senior Treasury executives are engaged in operational issues

[12] *Year 2000 Compliance Testing and Contingency Planning for Business Continuity at the United States Mint* (OIG-99-110) and *Monitoring of the United States Mint's Year 2000 Systems Compliance Testing and Contingency Planning for Business Continuity* (OIG-99-114).

[13] *Y2K Computing Challenge: Day One Planning and Operations Guide* (GAO/AIMD-10.1.22, issued in October 1999).

related to Y2K. The Department's efforts and additional actions needed to ensure the effectiveness of its Day One activities are described below:

EICC

In August 1999, the Department: developed standard operating procedures for the EICC and reporting requirements for the bureaus and offices to follow; identified the EICC needs and staff; developed alternate procedures in the event of problems, such as transmission failures; and held a "table top" reporting exercise with Y2K project officials from the Department and bureaus. At designated intervals during the rollover period, the EICC will receive from each Treasury bureau and office an assessment of their ability to perform core business processes and mission-critical IT, non-IT, and telecommunications systems.[14] The Department also developed and provided each bureau an automated program, ESY 2000, to enter the status reports and transmit them to the EICC through the Treasury email system.

Through the ESY 2000 application, EICC staff will collect, analyze, and summarize bureau status reports and produce, for each reporting period, an Executive Summary Report for approval by the EICC Director (the Assistant Secretary for Management and Chief Financial Officer or her designee). The Executive Summary Report will show for each bureau, and the Department as a whole, whether operations are "green" (core business processes are operating in a normal mode), "yellow" (core business processes are operating in a degraded mode, or components of the processes are unavailable), or "red" (core business processes cannot be performed). The Executive Summary Report will be the basis for reporting the status of the Department's operations to the President's Y2K Council.[15] It will also be posted on the Treasury intranet and provided to senior Treasury executives and others including the Chief of Staff, Under

[14] The Department has planned for the bureaus to report every 4 hours during the rollover period. Also, the bureaus have been instructed to submit "out of cycle" reports if there has been a significant change in their operational status.

[15] According to Office of Chief Information Officer staff, the Department has shared its reporting format with the President's Y2K Council. However, the President's Y2K Council had not developed a specific format for agencies to report their operational status during the Y2K rollover at the time of our review.

Secretaries, Assistant Secretaries, General Counsel, and the Department's Emergency Preparedness Team (EPT).[16]

The Department has conducted several tests of the ESY 2000 application, including a "dry run" on October 7, 1999, during which all the bureaus transmitted status reports to the EICC at designated intervals. As part of the dry run, which we observed, the bureaus included various failure scenarios in their reports and the Department's Y2K consultant produced Executive Summary Reports that were approved by the EICC Director's designated representative. As a result of these tests and our observations, the Department has made some modifications to the ESY 2000 application and identified other issues to be addressed. Specifically:

- More comprehensive tests of the EICC need to be performed. The October 7th dry run exercise was designed to test the ESY 2000 application. As such, it was not intended to test procedures for failure scenarios such as loss of power and communications, the inability of key EICC staff or the EICC Director to report for duty, or the need to transfer EICC operations to the backup facility. During our audit, we provided various EICC failure scenarios to the Department's Y2K project staff for its consideration in conducting future EICC tests. The Department has planned several more dry runs of the EICC including one scheduled for November 9, 1999. In its instructions for the November 9th dry run, the Department encouraged the bureaus to include scenarios such as staff not being available. The Department also plans to include a test of alternatives to the Treasury email system for communicating status reports during the November 9th dry run.

- Procedures need to be developed, and tested, to provide for an orderly transition from the primary EICC location to the backup facility if necessary.

- Procedures need to be developed, and tested, to transfer the EICC function to the EPT should circumstances warrant. In addition, a formal agreement/directive needs to be issued between the EPT and the EICC to document the responsibilities and trigger events if there is a need to engage the EPT.

[16] The EPT is responsible to have plans in place to respond to emergencies that could disrupt Treasury operations. According to Department officials, the EPT would use the EICC to conduct its operations if necessary during the century rollover.

- Designated bureau and office officials need to ensure the EICC receives status reports timely. During the October 7th dry run, one bureau did not submit its first report timely. Also, another bureau experienced problems transmitting to the EICC because its internal email system was not compatible with the Treasury email system.

- The EICC's contact list of responsible bureau and office officials needs to be current. When one bureau had not submitted its status report by the designated time during the October 7th dry run, EICC staff had to make multiple calls before reaching the correct person at the bureau.

- The Executive Summary Report needs to be revised to account for all bureaus and offices that are required to report to the EICC. We noted that only those bureaus that submitted reports appeared on the summary report. Including all bureaus on the summary report would ensure that the EICC Director and other senior Treasury executives are aware that a bureau had not reported its status, which may be indicative of the bureau experiencing a problem.

- Bureaus need to provide more detail when reporting on failed or degraded operations in order for the EICC Director to concur with the rating, determine whether further action is needed, and assign Treasury's overall status. For example, one bureau reported that an IT system was not working but did not state the nature of the impact to the related core business process. Since Treasury has over 300 mission-critical systems containing multiple sub-systems, the EICC Director may not be aware of all the systems by name and importance.

### Senior Treasury Executive Involvement

The Department has taken steps to ensure the involvement of senior Treasury executives during Day One. For example, executives will be at the EICC or otherwise available to receive the status reports and, if necessary, determine the appropriate action in the event a Treasury operation is negatively impacted by a Y2K incident. Additionally, senior Treasury executives met on October 20, 1999, to identify and examine operational issues associated with the year 2000 rollover. This meeting covered global issues that may affect Treasury's operations as well as EICC and Day One operations. Finally, the Department will be assigning a Treasury representative to be available to the President's Y2K Council at its government-wide Information Coordination Center.

**Recommendations**

4. The Deputy Assistant Secretary for Information Systems and Chief Information Officer should ensure that bureaus provide the Year 2000 Program Manager more complete information on the progress made to develop, test, and finalize business continuity and contingency plans for core business processes and supporting mission-critical IT and non-IT systems. As necessary, appropriate assistance should be provided to bureaus to ensure essential services will continue in the event of Y2K-induced failures of mission-critical systems.

   Management concurred with this recommendation.

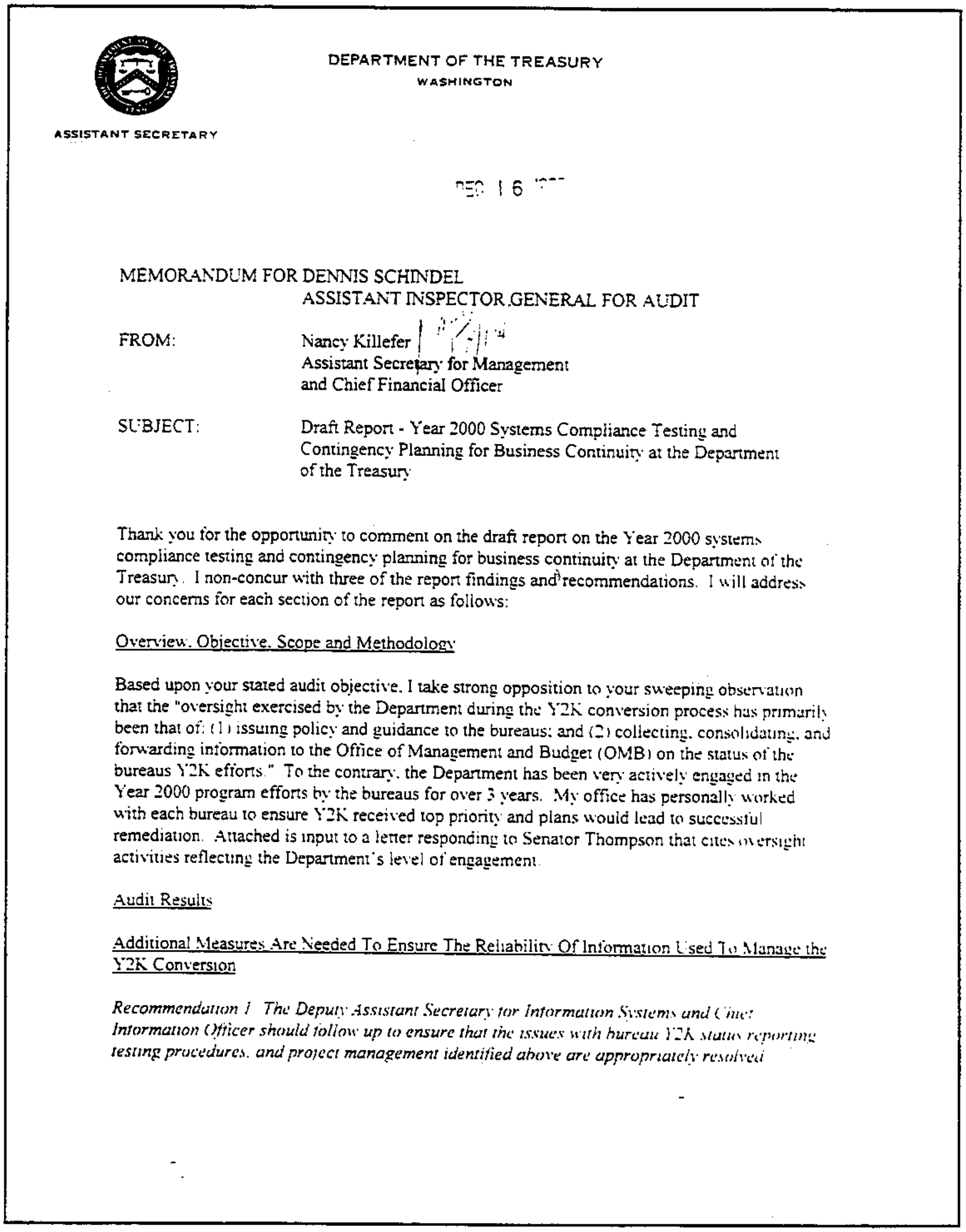
5. The Assistant Secretary for Management and Chief Financial Officer should ensure that planned tests of the EICC operations, including tests of the EICC backup facility consider: (1) unavailability of power, water, etc., at the EICC facility; (2) failure of the Department's email system to receive Day One bureau status reports from the bureaus; and (3) the inability of EICC staff and the EICC Director or designees to report for duty for their assigned shifts during the Day One rollover period. Furthermore, triggers for switching EICC operations to the backup facility should be developed. The EICC tests, including those of the backup facility, should be coordinated between the Deputy Assistant Secretary for Information Systems and Chief Information Officer and the Assistant Director (Emergency Preparedness) under the Deputy Assistant Secretary for Management Operations to ensure that the EICC will meet the needs of the Department's Emergency Preparedness Team.

   Management concurred with this recommendation.

## List of Abbreviations

| | |
|---|---|
| ATF | Bureau of Alcohol, Tobacco and Firearms |
| BCCP | Business Continuity and Contingency Plan |
| BEP | Bureau of Engraving and Printing |
| BPD | Bureau of Public Debt |
| CDN | Consolidated Data Network |
| CSM | Corporate Systems Management |
| Customs | United States Customs Service |
| Department | Department of the Treasury |
| EICC | Emergency Information Coordination Center |
| EPT | Emergency Preparedness Team |
| FMIS | Financial Management Information System (ATF) |
| FMS | Financial Management Service |
| GAO | U.S. General Accounting Office |
| IRS | Internal Revenue Service |
| IT | Information Technology |
| IV&V | Independent Verification and Validation |
| Mint | United States Mint |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| President's Y2K Council | President's Council for Year 2000 Conversion |
| SBU | Strategic Business Unit |
| SSA | Social Security Administration |
| STATS | Simplified Time and Attendance System |
| TCS | Treasury Communications System |
| Treasury | Department of the Treasury |
| Y2K | Year 2000 |
| Y2K PMO | Y2K Program Management Office (ATF) |
| Y2K SPO | Y2K Special Projects Office (FMS) |

# Management Response



DEPARTMENT OF THE TREASURY
WASHINGTON

ASSISTANT SECRETARY

DEC 16

MEMORANDUM FOR DENNIS SCHINDEL
ASSISTANT INSPECTOR GENERAL FOR AUDIT

FROM: Nancy Killefer
Assistant Secretary for Management
and Chief Financial Officer

SUBJECT: Draft Report - Year 2000 Systems Compliance Testing and Contingency Planning for Business Continuity at the Department of the Treasury

Thank you for the opportunity to comment on the draft report on the Year 2000 systems compliance testing and contingency planning for business continuity at the Department of the Treasury. I non-concur with three of the report findings and recommendations. I will address our concerns for each section of the report as follows:

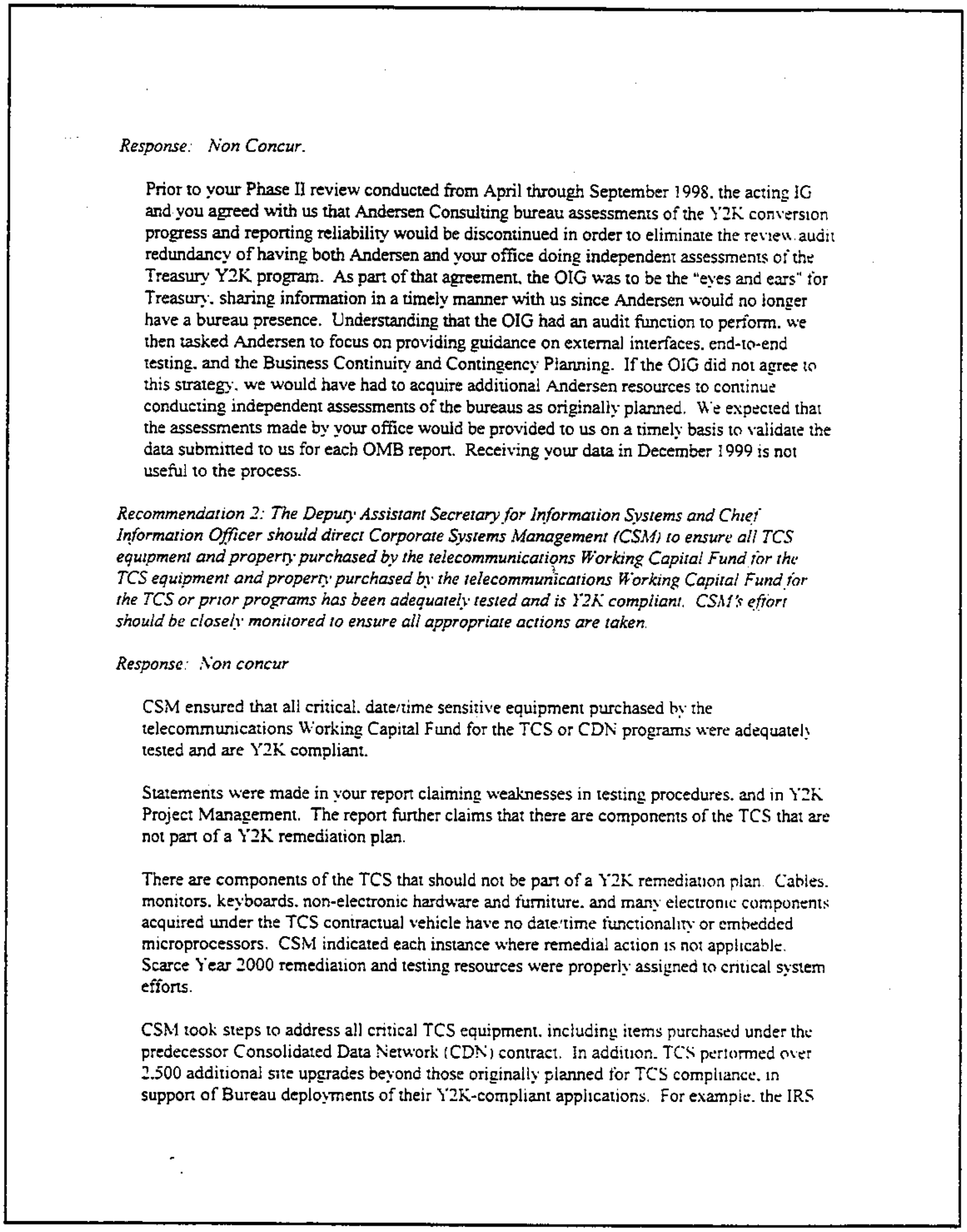
Overview, Objective, Scope and Methodology

Based upon your stated audit objective, I take strong opposition to your sweeping observation that the "oversight exercised by the Department during the Y2K conversion process has primarily been that of: (1) issuing policy and guidance to the bureaus; and (2) collecting, consolidating, and forwarding information to the Office of Management and Budget (OMB) on the status of the bureaus Y2K efforts." To the contrary, the Department has been very actively engaged in the Year 2000 program efforts by the bureaus for over 3 years. My office has personally worked with each bureau to ensure Y2K received top priority and plans would lead to successful remediation. Attached is input to a letter responding to Senator Thompson that cites oversight activities reflecting the Department's level of engagement.

Audit Results

Additional Measures Are Needed To Ensure The Reliability Of Information Used To Manage the Y2K Conversion

*Recommendation 1 The Deputy Assistant Secretary for Information Systems and Chief Information Officer should follow up to ensure that the issues with bureau Y2K status reporting testing procedures, and project management identified above are appropriately resolved*



*Response: Non Concur.*

Prior to your Phase II review conducted from April through September 1998, the acting IG and you agreed with us that Andersen Consulting bureau assessments of the Y2K conversion progress and reporting reliability would be discontinued in order to eliminate the review/audit redundancy of having both Andersen and your office doing independent assessments of the Treasury Y2K program. As part of that agreement, the OIG was to be the "eyes and ears" for Treasury, sharing information in a timely manner with us since Andersen would no longer have a bureau presence. Understanding that the OIG had an audit function to perform, we then tasked Andersen to focus on providing guidance on external interfaces, end-to-end testing, and the Business Continuity and Contingency Planning. If the OIG did not agree to this strategy, we would have had to acquire additional Andersen resources to continue conducting independent assessments of the bureaus as originally planned. We expected that the assessments made by your office would be provided to us on a timely basis to validate the data submitted to us for each OMB report. Receiving your data in December 1999 is not useful to the process.

*Recommendation 2: The Deputy Assistant Secretary for Information Systems and Chief Information Officer should direct Corporate Systems Management (CSM) to ensure all TCS equipment and property purchased by the telecommunications Working Capital Fund for the TCS equipment and property purchased by the telecommunications Working Capital Fund for the TCS or prior programs has been adequately tested and is Y2K compliant. CSM's effort should be closely monitored to ensure all appropriate actions are taken.*

*Response: Non concur*

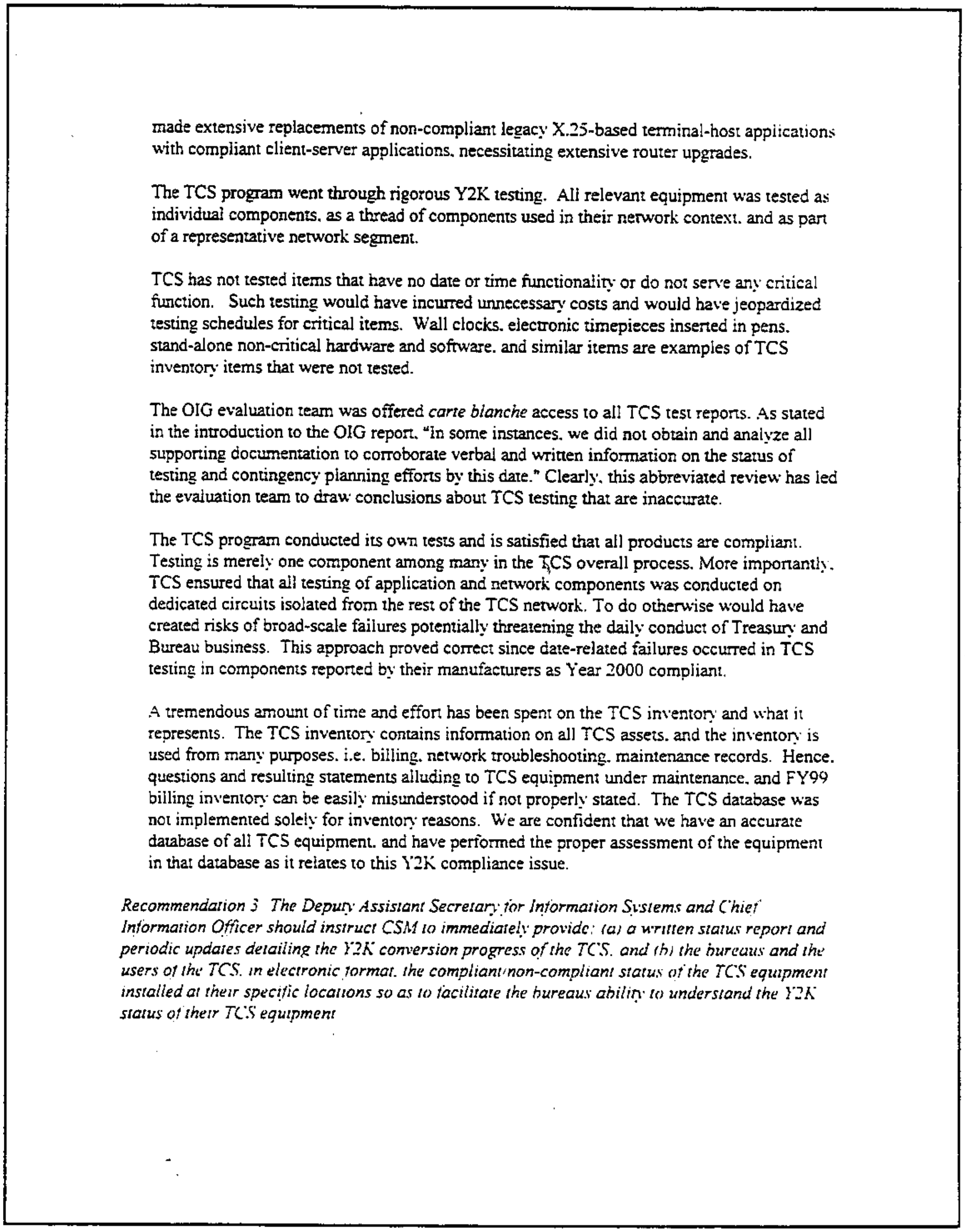
CSM ensured that all critical, date/time sensitive equipment purchased by the telecommunications Working Capital Fund for the TCS or CDN programs were adequately tested and are Y2K compliant.

Statements were made in your report claiming weaknesses in testing procedures, and in Y2K Project Management. The report further claims that there are components of the TCS that are not part of a Y2K remediation plan.

There are components of the TCS that should not be part of a Y2K remediation plan. Cables, monitors, keyboards, non-electronic hardware and furniture, and many electronic components acquired under the TCS contractual vehicle have no date/time functionality or embedded microprocessors. CSM indicated each instance where remedial action is not applicable. Scarce Year 2000 remediation and testing resources were properly assigned to critical system efforts.

CSM took steps to address all critical TCS equipment, including items purchased under the predecessor Consolidated Data Network (CDN) contract. In addition, TCS performed over 2,500 additional site upgrades beyond those originally planned for TCS compliance, in support of Bureau deployments of their Y2K-compliant applications. For example, the IRS

## Management Response



made extensive replacements of non-compliant legacy X.25-based terminal-host applications with compliant client-server applications, necessitating extensive router upgrades.

The TCS program went through rigorous Y2K testing. All relevant equipment was tested as individual components, as a thread of components used in their network context, and as part of a representative network segment.

TCS has not tested items that have no date or time functionality or do not serve any critical function. Such testing would have incurred unnecessary costs and would have jeopardized testing schedules for critical items. Wall clocks, electronic timepieces inserted in pens, stand-alone non-critical hardware and software, and similar items are examples of TCS inventory items that were not tested.

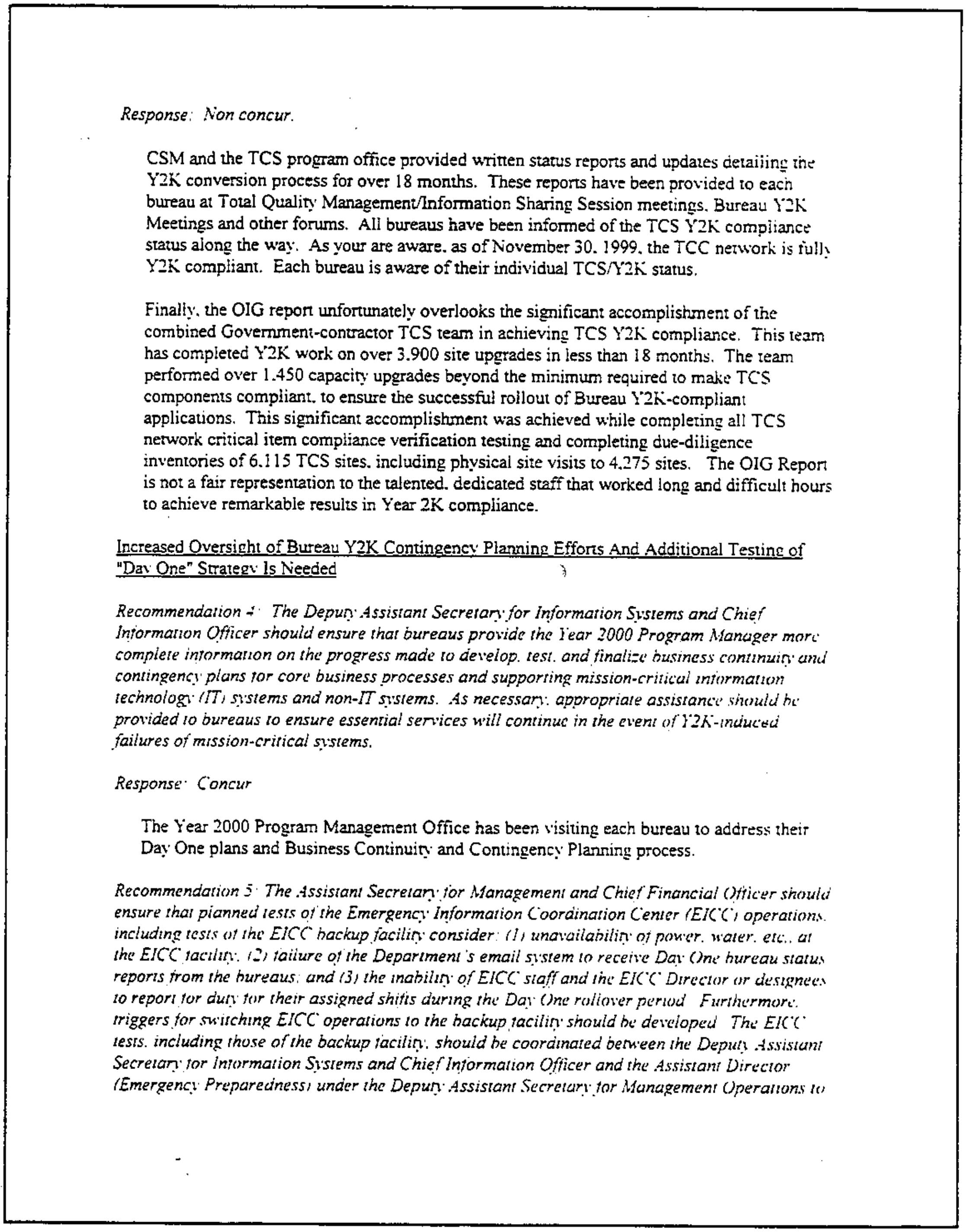
The OIG evaluation team was offered *carte blanche* access to all TCS test reports. As stated in the introduction to the OIG report, "In some instances, we did not obtain and analyze all supporting documentation to corroborate verbal and written information on the status of testing and contingency planning efforts by this date." Clearly, this abbreviated review has led the evaluation team to draw conclusions about TCS testing that are inaccurate.

The TCS program conducted its own tests and is satisfied that all products are compliant. Testing is merely one component among many in the TCS overall process. More importantly, TCS ensured that all testing of application and network components was conducted on dedicated circuits isolated from the rest of the TCS network. To do otherwise would have created risks of broad-scale failures potentially threatening the daily conduct of Treasury and Bureau business. This approach proved correct since date-related failures occurred in TCS testing in components reported by their manufacturers as Year 2000 compliant.

A tremendous amount of time and effort has been spent on the TCS inventory and what it represents. The TCS inventory contains information on all TCS assets, and the inventory is used from many purposes, i.e. billing, network troubleshooting, maintenance records. Hence, questions and resulting statements alluding to TCS equipment under maintenance, and FY99 billing inventory can be easily misunderstood if not properly stated. The TCS database was not implemented solely for inventory reasons. We are confident that we have an accurate database of all TCS equipment, and have performed the proper assessment of the equipment in that database as it relates to this Y2K compliance issue.

*Recommendation 3 The Deputy Assistant Secretary for Information Systems and Chief Information Officer should instruct CSM to immediately provide: (a) a written status report and periodic updates detailing the Y2K conversion progress of the TCS, and (b) the bureaus and the users of the TCS, in electronic format, the compliant/non-compliant status of the TCS equipment installed at their specific locations so as to facilitate the bureaus ability to understand the Y2K status of their TCS equipment*

## Management Response



*Response: Non concur.*

CSM and the TCS program office provided written status reports and updates detailing the Y2K conversion process for over 18 months. These reports have been provided to each bureau at Total Quality Management/Information Sharing Session meetings, Bureau Y2K Meetings and other forums. All bureaus have been informed of the TCS Y2K compliance status along the way. As your are aware, as of November 30, 1999, the TCC network is fully Y2K compliant. Each bureau is aware of their individual TCS/Y2K status.

Finally, the OIG report unfortunately overlooks the significant accomplishment of the combined Government-contractor TCS team in achieving TCS Y2K compliance. This team has completed Y2K work on over 3,900 site upgrades in less than 18 months. The team performed over 1,450 capacity upgrades beyond the minimum required to make TCS components compliant, to ensure the successful rollout of Bureau Y2K-compliant applications. This significant accomplishment was achieved while completing all TCS network critical item compliance verification testing and completing due-diligence inventories of 6,115 TCS sites, including physical site visits to 4,275 sites. The OIG Report is not a fair representation to the talented, dedicated staff that worked long and difficult hours to achieve remarkable results in Year 2K compliance.

Increased Oversight of Bureau Y2K Contingency Planning Efforts And Additional Testing of "Day One" Strategy Is Needed

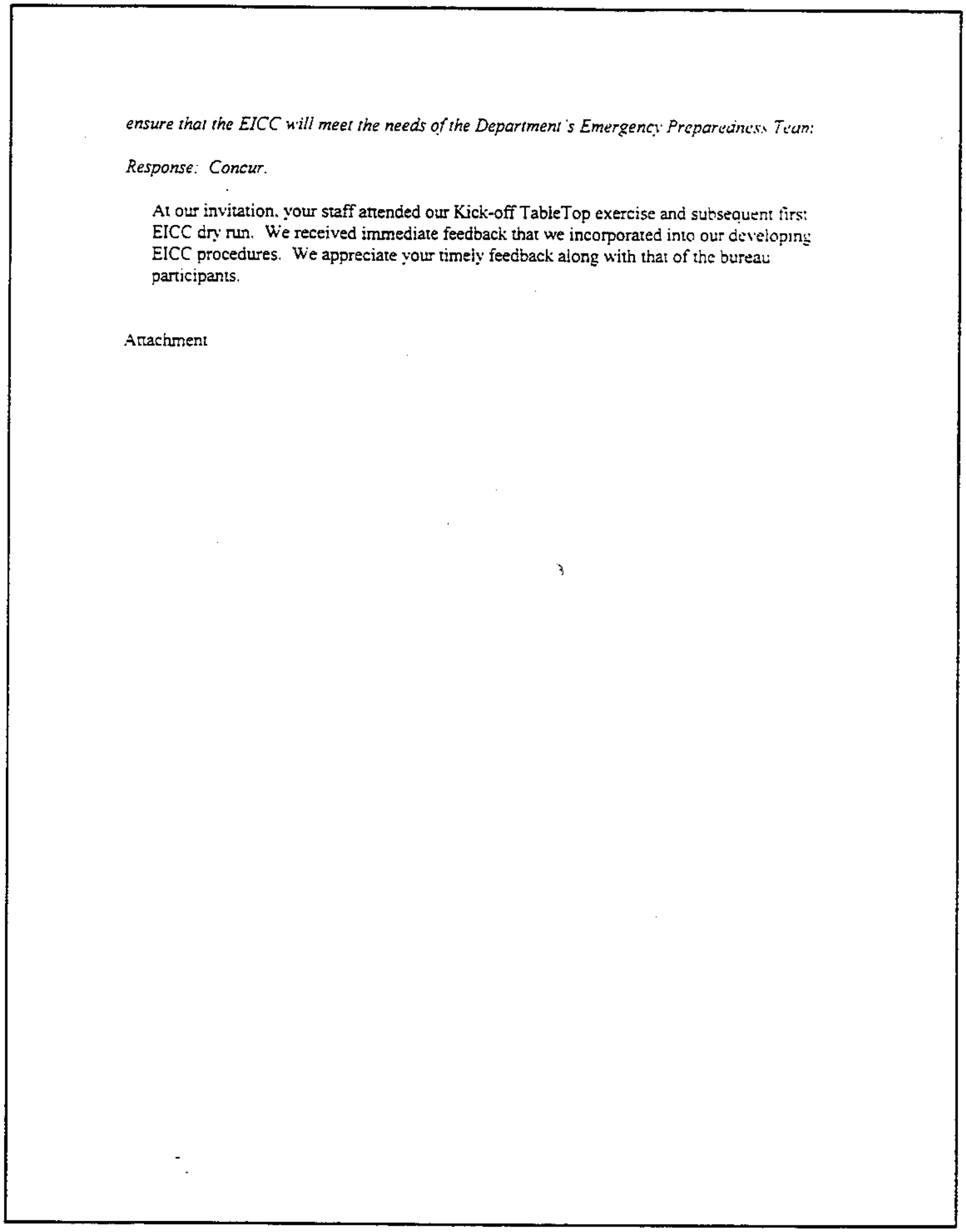
*Recommendation 4: The Deputy Assistant Secretary for Information Systems and Chief Information Officer should ensure that bureaus provide the Year 2000 Program Manager more complete information on the progress made to develop, test, and finalize business continuity and contingency plans for core business processes and supporting mission-critical information technology (IT) systems and non-IT systems. As necessary, appropriate assistance should be provided to bureaus to ensure essential services will continue in the event of Y2K-induced failures of mission-critical systems.*

*Response: Concur*

The Year 2000 Program Management Office has been visiting each bureau to address their Day One plans and Business Continuity and Contingency Planning process.

*Recommendation 5: The Assistant Secretary for Management and Chief Financial Officer should ensure that planned tests of the Emergency Information Coordination Center (EICC) operations, including tests of the EICC backup facility consider: (1) unavailability of power, water, etc., at the EICC facility, (2) failure of the Department's email system to receive Day One bureau status reports from the bureaus; and (3) the inability of EICC staff and the EICC Director or designees to report for duty for their assigned shifts during the Day One rollover period. Furthermore, triggers for switching EICC operations to the backup facility should be developed. The EICC tests, including those of the backup facility, should be coordinated between the Deputy Assistant Secretary for Information Systems and Chief Information Officer and the Assistant Director (Emergency Preparedness) under the Deputy Assistant Secretary for Management Operations to*

## Management Response



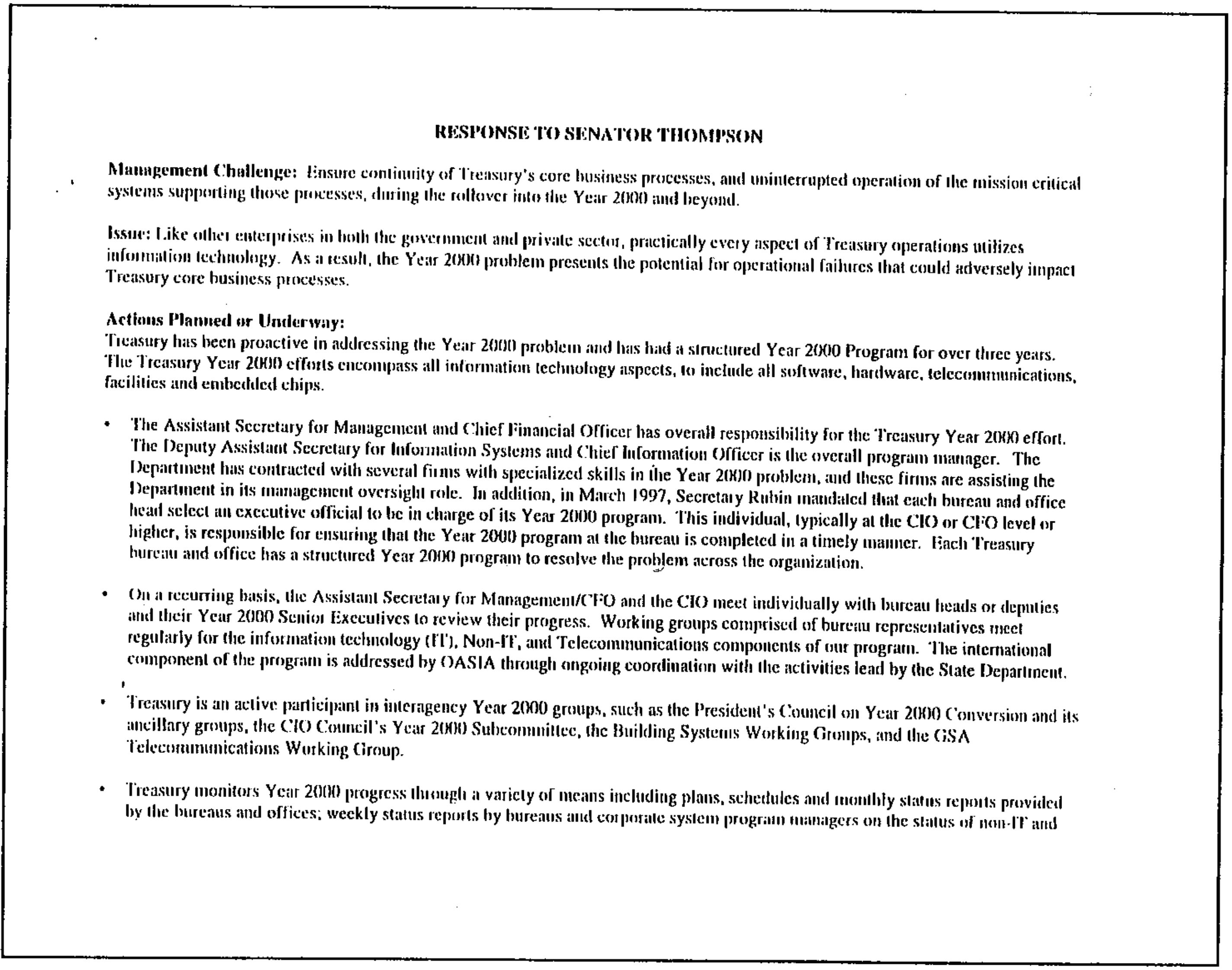
*ensure that the EICC will meet the needs of the Department's Emergency Preparedness Team:*

*Response: Concur.*

At our invitation, your staff attended our Kick-off TableTop exercise and subsequent first EICC dry run. We received immediate feedback that we incorporated into our developing EICC procedures. We appreciate your timely feedback along with that of the bureau participants.

Attachment

## Management Response



**RESPONSE TO SENATOR THOMPSON**

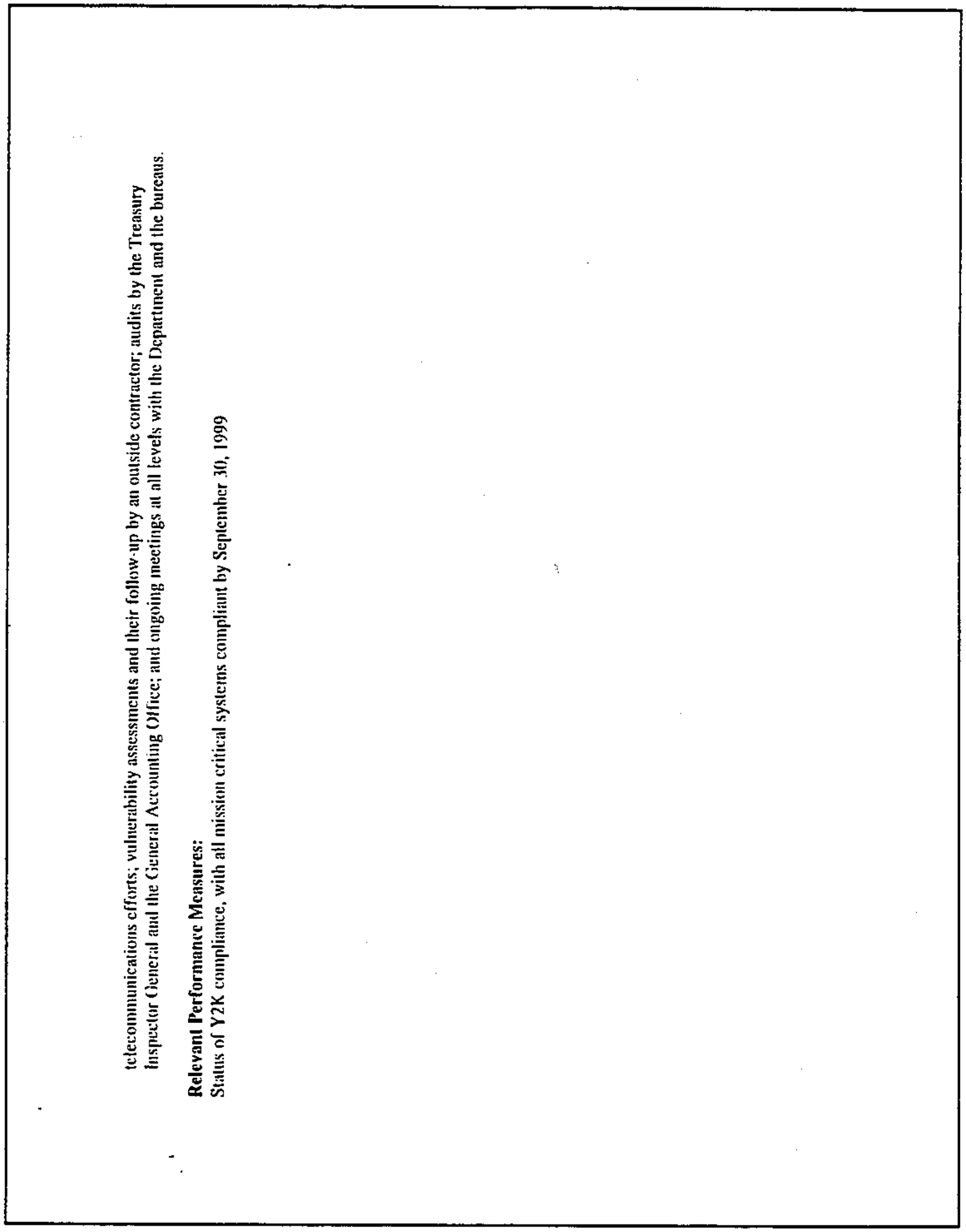
**Management Challenge:** Ensure continuity of Treasury's core business processes, and uninterrupted operation of the mission critical systems supporting those processes, during the rollover into the Year 2000 and beyond.

**Issue:** Like other enterprises in both the government and private sector, practically every aspect of Treasury operations utilizes information technology. As a result, the Year 2000 problem presents the potential for operational failures that could adversely impact Treasury core business processes.

**Actions Planned or Underway:**
Treasury has been proactive in addressing the Year 2000 problem and has had a structured Year 2000 Program for over three years. The Treasury Year 2000 efforts encompass all information technology aspects, to include all software, hardware, telecommunications, facilities and embedded chips.

- The Assistant Secretary for Management and Chief Financial Officer has overall responsibility for the Treasury Year 2000 effort. The Deputy Assistant Secretary for Information Systems and Chief Information Officer is the overall program manager. The Department has contracted with several firms with specialized skills in the Year 2000 problem, and these firms are assisting the Department in its management oversight role. In addition, in March 1997, Secretary Rubin mandated that each bureau and office head select an executive official to be in charge of its Year 2000 program. This individual, typically at the CIO or CFO level or higher, is responsible for ensuring that the Year 2000 program at the bureau is completed in a timely manner. Each Treasury bureau and office has a structured Year 2000 program to resolve the problem across the organization.
- On a recurring basis, the Assistant Secretary for Management/CFO and the CIO meet individually with bureau heads or deputies and their Year 2000 Senior Executives to review their progress. Working groups comprised of bureau representatives meet regularly for the information technology (IT), Non-IT, and Telecommunications components of our program. The international component of the program is addressed by OASIA through ongoing coordination with the activities lead by the State Department.
- Treasury is an active participant in interagency Year 2000 groups, such as the President's Council on Year 2000 Conversion and its ancillary groups, the CIO Council's Year 2000 Subcommittee, the Building Systems Working Groups, and the GSA Telecommunications Working Group.
- Treasury monitors Year 2000 progress through a variety of means including plans, schedules and monthly status reports provided by the bureaus and offices; weekly status reports by bureaus and corporate system program managers on the status of non-IT and

## Management Response



telecommunications efforts; vulnerability assessments and their follow-up by an outside contractor; audits by the Treasury Inspector General and the General Accounting Office; and ongoing meetings at all levels with the Department and the bureaus.

**Relevant Performance Measures:**
Status of Y2K compliance, with all mission critical systems compliant by September 30, 1999

## Major Contributors to This Report

Clifford Jennings, Director, Office of Information Technology Audits
Ed Coleman, Deputy Director, Office of Information Technology Audits
Robert Taylor, IT Audit Manager
Jean Purcell, Audit Manager
Melinda Rose, IT Auditor
Catherine Fudge, IT Auditor
Ethel Taylor-Young, Auditor
Kevin Burke, IT Auditor
Joey Maranto, IT Auditor
LaVeta Charity, Auditor
Michael DiDiego, IT Auditor
Charles Intrabartolo, Computer Specialist
Inez Jordan, Auditor
Michael Stein, IT Auditor
Michael Sielicki, Auditor
Luis Reyes, Referencer
Valarie Moore, Referencer
Ehab Bestawrose, Referencer

## Report Distribution

### Treasury Departmental Offices

Assistant Secretary for Management and Chief Financial Officer
Deputy Assistant Secretary for Information Systems and Chief Information Officer
Assistant Director of Information Technology Policy and Management
Deputy Assistant Secretary for Management Operations
Assistant Director, (Emergency Preparedness)
Director, Corporate Systems Management
Director, Executive Office for Asset Forfeiture
Office of Budget
Director, Office of Strategic Planning and Evaluations
Director, Office of Accounting and Internal Control
CIO Liaison, Business Services Division

### Office of Management and Budget

Esther Rosenbaum, Budget Examiner